(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 318 283 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
07.02.2024 Bulletin 2024/06

(21) Application number: **22773954.7**

(22) Date of filing: **18.02.2022**

(51) International Patent Classification (IPC):
G06F 21/56 *(2013.01)*

(86) International application number:
PCT/CN2022/076785

(87) International publication number:
WO 2022/199292 (29.09.2022 Gazette 2022/39)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **26.03.2021 CN 202110323745**

(71) Applicant: **Alipay (Hangzhou) Information Technology Co., Ltd.**
Hangzhou, Zhejiang 310000 (CN)

(72) Inventors:
- **CAO, Shijie**
  Hangzhou, Zhejiang 310000 (CN)
- **LI, Wenjie**
  Hangzhou, Zhejiang 310000 (CN)
- **ZHAO, Hao**
  Hangzhou, Zhejiang 310000 (CN)

(74) Representative: **Winter, Brandl - Partnerschaft mbB**
Alois-Steinecker-Straße 22
85354 Freising (DE)

(54) DETECTION OF MALICIOUS BEHAVIOR OF APPLET

(57) Some embodiments of this specification provide a method and an apparatus for detecting a malicious behavior of an applet. According to the method in some embodiments, first, at least two behavior records that are generated through triggering during running of the applet are obtained; then, a behavior feature of each behavior record is extracted; next, at least one feature combination is formed by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features; and finally, it is determined whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, it is determined that the applet conducts a malicious behavior.

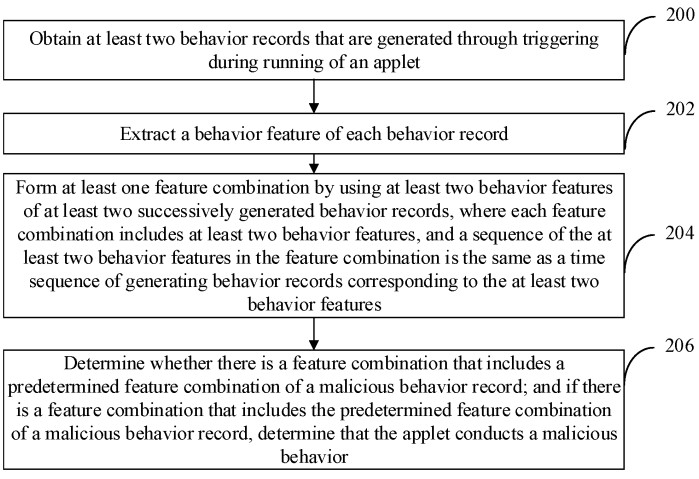

FIG. 2

EP 4 318 283 A1

Description

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to the field of computer technologies, and in particular, to detection of a malicious behavior of an applet.

BACKGROUND

[0002] An applet is an application that can be used without downloading and installing. Generally, the applet needs to rely on a specific applet platform (other application software), and implements its service functions through a service interface provided by the applet platform. A malicious applet causes problems such as leakage of privacy data of a user and a property loss. Therefore, how to detect whether an applet conducts a malicious behavior becomes a focus of attention of program developers.

[0003] In a conventional technology, security scanning is performed on static code of an applet to detect whether a malicious behavior exists in the static code. However, the conventional technology solution encounters a problem of low detection accuracy. Therefore, it is necessary to provide a more reliable method for detecting a malicious behavior of an applet.

SUMMARY

[0004] One or more embodiments of this specification describe a method and an apparatus for detecting a malicious behavior of an applet, so as to improve accuracy of detecting a malicious behavior of an applet.

[0005] According to a first aspect, a method for detecting a malicious behavior of an applet is provided, including: obtaining at least two behavior records that are generated through triggering during running of the applet; extracting a behavior feature of each behavior record; forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features; determining whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, determining that the applet conducts a malicious behavior.

[0006] In some embodiments, the behavior record includes at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

[0007] In some embodiments, the obtaining at least two behavior records that are generated through triggering during running of the applet includes: obtaining at least two behavior records generated by the applet during running of the applet; and the forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records includes: forming one feature combination by using behavior features of the at least two behavior records generated by the applet.

[0008] In some embodiments, the obtaining at least two behavior records that are generated through triggering during running of the applet includes: obtaining at least two behavior records generated by the applet during running of the applet; for two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determining whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generating a corresponding behavior record for the third function page; and using the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

[0009] In some embodiments, the forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records includes: forming a first feature combination by using behavior features of the at least two behavior records generated by the applet; and forming at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

[0010] In some embodiments, the obtaining at least two behavior records generated by the applet during running of the applet includes: obtaining at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet.

[0011] In some embodiments, the extracting a behavior feature of each behavior record includes: determining, based on a name, included in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determining a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determining the determined classification value as the behavior feature of the behavior record; and/or detecting, based on parameter information, included in the behavior record, in an invoking request sent

by the applet and parameter information, included in the behavior record, in an invoking request response received by the applet, privacy data included in the parameter information; determining, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determining the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

[0012] According to a second aspect, an apparatus for detecting a malicious behavior of an applet is provided, including: a behavior record obtaining unit, configured to obtain at least two behavior records that are generated through triggering during running of the applet; a behavior feature extraction unit, configured to extract a behavior feature of each behavior record; a feature combination unit, configured to form at least one feature combination by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features; and a determining unit, configured to determine whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, determine that the applet conducts a malicious behavior.

[0013] In some embodiments, the behavior record includes at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

[0014] In some embodiments, the behavior record obtaining unit is configured to obtain at least two behavior records generated by the applet during running of the applet; and the feature combination unit is configured to form one feature combination by using behavior features of the at least two behavior records generated by the applet.

[0015] In some embodiments, the behavior record obtaining unit is configured to: obtain at least two behavior records generated by the applet during running of the applet; for two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determine whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generate a corresponding behavior record for the third function page; and use the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

[0016] In some embodiments, the feature combination unit is configured to form a first feature combination by using behavior features of the at least two behavior records generated by the applet; and form at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

[0017] In some embodiments, the behavior record obtaining unit is configured to: when obtaining the at least two behavior records generated by the applet during running of the applet, obtain at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet.

[0018] In some embodiments, the behavior feature extraction unit is configured to determine, based on a name, included in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determine a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determine the determined classification value as the behavior feature of the behavior record; and/or detect, based on parameter information, included in the behavior record, in an invoking request sent by the applet and parameter information, included in the behavior record, in an invoking request response received by the applet, privacy data included in the parameter information; determine, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determine the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

[0019] According to a third aspect, a computer-readable storage medium is provided, where the computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the method according to any embodiment of this specification.

[0020] According to a fourth aspect, a computing device is provided, including a memory and a processor, where the memory stores executable code, and the processor executes the executable code to implement the method according to any embodiment of this specification.

[0021] In the method and apparatus for detecting a malicious behavior of an applet provided in some embodiments of this specification, at least two behavior records that are generated through triggering during running of the applet are obtained; a behavior feature of each behavior record is extracted; then at least one feature combination is formed by using at least two behavior features

of at least two successively generated behavior records; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, it is determined that the applet conducts a malicious behavior. This solution is to detect whether there is a malicious behavior in a plurality of consecutive invoking behaviors of the applet, providing high coverage of invoking behaviors, and therefore can improve accuracy of detecting a malicious behavior of the applet.

BRIEF DESCRIPTION OF DRAWINGS

[0022] To describe the technical solutions in some embodiments of this specification or in a conventional technology more clearly, the following briefly describes the accompanying drawings needed for describing some embodiments or the conventional technology. Clearly, the accompanying drawings in the following descriptions show some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

FIG. 1 is a schematic diagram of a system architecture according to some embodiments of this specification;

FIG. 2 is a flowchart of a method for detecting a malicious behavior of an applet according to some embodiments of this specification;

FIG. 3 is a flowchart of obtaining a behavior record according to some embodiments of this specification;

FIG. 4 is a schematic diagram of a behavior record according to some embodiments of this specification;

FIG. 5 is a flowchart of obtaining a behavior record according to some other embodiments of this specification;

FIG. 6 is a schematic diagram of a behavior graph according to some embodiments of this specification; and

FIG. 7 is a structural diagram of an apparatus for detecting a malicious behavior of an applet according to some embodiments of this specification.

DESCRIPTION OF EMBODIMENTS

[0023] The solutions provided in this specification are described below with reference to the accompanying drawings.

[0024] In a conventional technology, security scanning is performed on static code of an applet to detect whether a malicious behavior exists in the static code. For example, it is detected whether a service interface of a fixed feature is invoked in the static code, and whether there is leakage of sensitive information when the service interface is invoked. The conventional technology is to detect whether an invoking behavior of a single service interface is malicious. However, during actual running, the applet conducts a plurality of consecutive invoking behaviors, and there is a malicious behavior in the plurality of consecutive invoking behaviors. For example, the applet sends sensitive data of the user to the outside by invoking a combination of a plurality of different service interfaces, but there is a reasonable service requirement for invoking a single service interface. In such case, in the conventional technology, a malicious behavior of the applet cannot be detected, causing low detection accuracy. Therefore, it may be considered according to this solution that, a behavior record of an applet during running is obtained, and an existing malicious sample is used to detect the behavior record of the applet, so as to determine whether the applet conducts a malicious behavior.

[0025] The following describes some specific implementations of the above-mentioned ideas.

[0026] To facilitate understanding of this specification, a system architecture used in this specification is first described. As shown in FIG. 1, the system architecture mainly includes a client and a server.

[0027] An application that can serve as a host application of each applet is installed in the client. An APP in the client shown in FIG. 1 is a host application. By using a bridging (JavaScript Bridge) mechanism, the host application provides a service interface (JSAPI) that can be invoked for each applet, and each applet implements a corresponding service function by invoking each service interface. For example, the host application is "Alipay", and the applet is "Cainiao", "Travel", or "Eleme" .

[0028] The client may be an intelligent device located on a user side, for example, a mobile phone, a tablet computer, or a notebook computer.

[0029] The server may be a server that provides a service for the host application or the client.

[0030] FIG. 2 is a flowchart of a method for detecting a malicious behavior of an applet according to some embodiments. It may be understood that the method can be performed by any apparatus, device, platform, or device cluster having computing and processing capabilities. Referring to FIG. 2, subsequent specific implementation includes:

Step 200: Obtain at least two behavior records that are generated through triggering during running of the applet.

Step 202: Extract a behavior feature of each behavior record.

Step 204: Form at least one feature combination by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features.

Step 206: Determine whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, determine that the applet conducts a malicious behavior.

[0031] In the method for detecting a malicious behavior of an applet shown in FIG. 2, at least two behavior records that are generated through triggering during running of the applet are obtained; a behavior feature of each behavior record is extracted; then at least one feature combination is formed by using at least two behavior features of at least two successively generated behavior records; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, it is determined that the applet conducts a malicious behavior. This solution is to detect whether there is a malicious behavior in a plurality of consecutive invoking behaviors of the applet, providing high coverage of invoking behaviors, and therefore can improve accuracy of detecting a malicious behavior of the applet.

[0032] The following describes a method for performing each step shown in FIG. 2.

[0033] For step 200, at least two behavior records that are generated through triggering during running of the applet are obtained.

[0034] In some embodiments of this specification, in step 200, a behavior record is generated through triggering during running of the applet, and the at least two behavior records that are generated through triggering correspond to at least the following two cases.

[0035] Case 1: The at least two behavior records include at least two behavior records generated by the applet during running of the applet.

[0036] Case 2: The at least two behavior records include at least two behavior records generated by the applet during running of the applet, and a behavior record generated based on the at least two behavior records generated by the applet.

[0037] The following separately describes the behavior record obtaining method in some embodiments of this specification for the above-mentioned two cases.

[0038] For case 1:

In case 1, FIG. 3 is a flowchart of obtaining a behavior record according to some embodiments of this specification. Referring to FIG. 3, step 200 may specifically include step 300: Obtain at least two behavior records generated by the applet during running of the applet.

[0039] In step 300, obtaining at least two behavior records generated by the applet during running of the applet may be obtaining at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet. For example, the applet generates a behavior record when invoking a service interface with a file uploading function, and the applet generates a behavior record when invoking a service interface with a file downloading function.

[0040] It may be understood that the behavior record is generated by the applet when invoking a service interface during running, or can be generated by the applet when executing corresponding logic based on static code corresponding to the applet during running.

[0041] In some embodiments of this specification, the behavior record may include at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

[0042] FIG. 4 is a schematic diagram of a plurality of behavior records that are generated by the applet during running of the applet and that are obtained by a server. A first behavior record is used as an example to describe content included in the behavior record. In the first behavior record, a name of a service interface invoked by the applet is GetUserInfo; a time at which the applet invokes the service interface is 15:00:00; parameter information in an invoking request sent by the applet is a parameter 1; parameter information in an invoking request response received by the applet is a return result 1; a function page corresponding to the applet after invoking the service interface is a function page 1.

[0043] For case 2:

In case 2, FIG. 5 is another flowchart of obtaining a behavior record according to some embodiments of this specification. Referring to FIG. 5, step 200 may specifically include step 500: Obtain at least two behavior records generated by the applet during running of the applet.

[0044] An execution process of step 500 is the same as that of step 300. For description of step 500, references are made to the description of step 300, and details are not described herein again.

[0045] Step 502: For two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determine whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generate a corresponding behavior record for the third function page.

[0046] The two adjacent behavior records in this step are two behavior records at adjacent locations after at least two behavior records obtained in step 500 are sorted based on a time sequence of generating the behavior records.

[0047] Each behavior record corresponds to one function page. For example, after invoking a service interface 1, the applet enters a function page 1, and when the

applet invokes a service interface 2 on the function page 1, the applet enters a function page 2 after invoking the service interface 2. In addition, it may be understood, based on content included in the behavior record, that information about a function page corresponding to the applet after invoking a service interface may be located in the behavior record.

[0048] This step is described by using a behavior record 1 and a behavior record 2 that are adjacent to each other in the at least two behavior records obtained in step 500 as examples. The behavior record 1 corresponds to the function page 1, the behavior record 2 corresponds to the function page 2, and a generation time of the behavior record 1 is earlier than a generation time of the behavior record 2.

[0049] It may be understood that the server can pre-store a relationship between function pages of the applet. It can be determined based on a relationship between the function page 1 and the function page 2 that, when the applet jumps from the function page 1 to the function page, in addition to directly jumping from the function page 1 to the function page 2, the applet can jump to the function page 2 via a function page 1A1 and a function page 1A2, or can jump to the function page 2 via a function page 1B1, that is, there are the following three paths from the function page 1 to the function page 2:

Path 1: function page 1 -> function page 2;
Path 2: function page 1 -> function page 1A1 -> function page 1A2 -> function page 2;
Path 3: function page 1 -> function page 1B1 -> function page 2.

[0050] In such case, corresponding behavior records need to be generated for the function page 1A1, the function page 1A2, and the function page 1B1, respectively.

[0051] When the corresponding behavior record is generated for the third function page, the corresponding behavior record can be generated based on a pre-stored mapping relationship between the function page and the service interface, and parameter information corresponding to invoking the service interface and returning the invoking request response. It should be noted that the generation time of the behavior record corresponding to the third function page needs to be located between the first function page and the second function page. The path 2 is used as an example. Generation times of behavior records corresponding to the function pages included in the path 2 are successively the function page 1, the function page 1A1, the function page 1A2, and the function page 2.

[0052] Step 504: Use the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

[0053] It is determined whether there is a transit third function page between the first function page and the second function page that respectively correspond to the two adjacent behavior records, and a corresponding behavior record is generated for the transit third function page. Then, the behavior record generated for the third function page and the at least two behavior records generated by the applet are used together as the at least two behavior records that are generated through triggering during running of the applet. As such, the behavior record used to detect whether the applet conducts a malicious behavior is more abundant, and further detection accuracy is higher when the more abundant behavior record is used to analyze whether the applet conducts a malicious behavior.

[0054] Regardless of case 1 or case 2, in some embodiments of this specification, a behavior record generated through triggering during running of the applet can be obtained and sent by a client.

[0055] It may be understood from the foregoing description of the system architecture to which this specification is applicable that, by using the bridging mechanism, the host application provides a service interface that can be invoked for each applet. When invoking a service interface, the applet sends an invoking request to the JavaScript Bridge according to an agreed protocol, where the invoking request includes the carried parameter information and the information about the service interface that needs to be invoked. Then, the host application invokes the service interface based on the information about the service interface, so as to return an invoking request response to the applet. Therefore, the client can obtain at least two behavior records generated when the applet invokes at least two service interfaces during running.

[0056] In some embodiments of this specification, the client can obtain a behavior record by using a security aspect module. Specifically, the JavaScript Bridge can be cut by using a Hook (hook function) or through static code replacement, so that when sending an invoking request to the JavaScript Bridge, the applet first routes execution logic to a security aspect module. The security aspect module receives the invoking request, and forwards the invoking request to the JavaScript Bridge. When the JavaScript Bridge sends an invoking request response to the security aspect module, the security aspect module sends the invoking request response to the applet. As such, the security aspect module can obtain the behavior record generated when the applet invokes the service interface.

[0057] The aspect means aspect-oriented programming (AOP), which is a programming paradigm that dynamically adds a function to a program without modifying source code through pre-compilation, dynamic runtime proxy, or injection. Therefore, the invoking request and the invoking request response are obtained by using the security aspect module, so that an invoking behavior of the applet for the service interface can be monitored, and the invoking behavior is recorded without affecting a service function to be implemented by the applet.

[0058] For step 202, the behavior feature of each behavior record is extracted.

[0059] In some embodiments of this specification, the behavior feature can be extracted separately based on at least the following two dimensions.

[0060] Dimension 1: The function of the service interface corresponding to the behavior record.

[0061] Dimension 2: Sensitivity of data corresponding to the behavior record.

[0062] The following describes extraction of the behavior feature separately based on the above-mentioned two dimensions.

[0063] In terms of dimension 1, step 202 may include: determining, based on a name, included in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determining a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determining the determined classification value as the behavior feature of the behavior record.

[0064] In some embodiments of this specification, all service interfaces that can be provided by the host application can be classified in advance based on service functions implemented by the service interfaces. For example, the classification may include a file operation type, a network operation type, a device information type, and the like. A classification value is defined for each classification. For example, a classification value corresponding to the file operation type is 1, a classification value corresponding to the network operation type is 2, and a classification value corresponding to the device information type is 3.

[0065] It may be understood that a mapping relationship among a service interface name, a classification, and a classification value is stored in the server. In such case, when a behavior feature is extracted for a behavior record, a classification value can be determined directly based on the name of the service interface invoked by the applet and the stored mapping relationship that are included in the behavior record, and the determined classification value is determined as the behavior feature of the behavior record.

[0066] It should be noted that, in terms of dimension 1, in addition to the above-mentioned definition of a classification value for a classification, there may be another form of definition. For example, a classification granularity is further divided. In an example in which functions of service interfaces included in the file operation type are uploading a file, downloading a file, obtaining a file path, and the like, corresponding classification values can be respectively defined for uploading a file, downloading a file, and obtaining a file path in the file operation type. After the classification value is used as an extracted behavior feature, when the behavior feature is used to detect whether the applet conducts a malicious behavior, detection accuracy is further improved.

[0067] In terms of dimension 2, step 202 may include: detecting, based on parameter information, included in the behavior record, in an invoking request sent by the applet and parameter information, included in the behavior record, in an invoking request response received by the applet, privacy data included in the parameter information; determining, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determining the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

[0068] In some embodiments of this specification, an applet may involve privacy data when invoking a service interface, and there is a specific relationship between a malicious behavior of the applet and privacy data. Therefore, the behavior feature can be extracted by using the sensitivity of the corresponding data in the behavior record as a dimension.

[0069] In some embodiments of this specification, the server can predefine a data type of the privacy data, and define a sensitivity weight value of each data type. The data type may include location information, a user ID, identity information, a file name, and the like. A sensitivity weight value can be defined for each data type based on a sensitive program of data corresponding to the data type. For example, the sensitivity weight value of the identity information is larger than the sensitivity weight value of the location information.

[0070] It may be understood that a mapping relationship between each data type and a sensitivity weight value is stored in the server. In such case, when a behavior feature is extracted for a behavior record, it can be detected, directly based on parameter information (parameter information in an invoking request sent by the applet and parameter information in an invoking request response received by the applet) included in the behavior record, whether the parameter information includes privacy data, and a data type of the privacy data is determined. Then, a sensitivity weight value corresponding to the privacy data is determined based on the mapping relationship between each data type and the sensitivity weight value stored in the server.

[0071] It should be noted that, in terms of dimension 2, if the parameter information in the behavior record includes a plurality of pieces of privacy data, a comprehensive sensitivity weight value of the behavior record can be calculated by using a sensitivity weight value of each piece of privacy data, and the comprehensive sensitivity weight value is determined as the behavior feature of the behavior record.

[0072] There may be a plurality of methods for calculating the comprehensive sensitivity weight value, for example, adding up the sensitivity weight values of all pieces of privacy data, or dividing a sum of the sensitivity weight values of all pieces of privacy data by a quantity of pieces of privacy data.

[0073] In some preferred embodiments of this specification, the classification values and sensitivity weight val-

ues that are respectively determined in terms of the above-mentioned two dimensions are all used as behavior features of the behavior record. When the behavior features in these preferred embodiments are used to compare and determine a subsequent feature combination, the behavior features can be determined to be the same only when both the classification values and the sensitivity weight values are the same. As such, an analysis granularity is more refined, thereby further improving detection accuracy.

[0074] In some embodiments of this specification, the behavior feature is quantized into a numerical form, and when the behavior feature in the numerical form is used to compare and determine a subsequent feature combination, whether the behavior features are the same can be determined directly by comparing whether values are equal. As such, the determining and comparison processes are more convenient, thereby increasing a speed of detecting a malicious behavior of an applet.

[0075] For step 204, at least one feature combination is formed by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features.

[0076] In some embodiments of this specification, when the at least two behavior records that are generated through triggering during running of the applet in step 200 correspond to different cases, the feature combination formed in step 204 varies. The following separately describes the two cases.

[0077] When the at least two behavior records that are generated through triggering during running of the applet in step 200 correspond to case 1, step 204 may include: forming one feature combination by using behavior features of the at least two behavior records generated by the applet.

[0078] For example, it can be determined based on step 200 that, a sequence of the generation times of the behavior records is as follows: behavior record 1, behavior record 2, behavior record 3, ..., and behavior record n, where n is an integer not less than 2. Behavior feature 1, behavior feature 2, behavior feature 3, ..., and behavior feature n can be successively extracted based on step 202. In such case, a feature combination formed in step 204 is as follows: behavior feature 1, behavior feature 2, behavior feature 3, ..., and behavior feature n.

[0079] When the at least two behavior records that are generated through triggering during running of the applet in step 200 correspond to case 2, step 204 may include: forming a first feature combination by using behavior features of the at least two behavior records generated by the applet; and forming at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

[0080] For example, it can be determined based on step 200 that, a sequence of the generation times of the behavior records is as follows: behavior record 1, behavior record 2, behavior record 3, ..., and behavior record n, where n is an integer not less than 2. In addition, the function page 1 corresponding to the behavior record 1 can alternatively jump to the function page 2 corresponding to the behavior record 2 via a function page 1A1, and the function page 2 corresponding to the behavior record 2 can alternatively jump to the function page 3 corresponding to the behavior record 3 via a function page 2A1. In such case, a behavior record 1A1 and a behavior record 2A1 are generated for the function page 1A1 and the function page 2A1. Behavior feature 1, behavior feature 1A1, behavior feature 2, behavior feature 2A1, behavior feature 3, ..., and behavior feature n can be successively extracted based on step 202.

[0081] During formation of the feature combination, to help determine a quantity of feature combinations that can be formed, a behavior graph of the applet can be first restored. FIG. 6 is a schematic diagram of a behavior graph disclosed in some embodiments of this specification. The behavior graph includes behavior nodes and an edge relationship between behavior nodes, and a behavior node corresponds to a behavior record. According to the behavior graph, four behavior links can be obtained: behavior node 1 -> behavior node 2 -> behavior node 3, ..., and behavior node n; behavior node 1 -> behavior node 2 -> behavior node 2A1 -> behavior node 3, ..., and behavior node n; behavior node 1 -> behavior node 1A1 -> behavior node 2 -> behavior node 3, ..., and behavior node n; behavior node 1 -> behavior node 1A1 -> behavior node 2 -> behavior node 2A1 -> behavior node 3, ..., and behavior node n.

[0082] In such case, the four behavior links obtained above can form four feature combinations in step 204.

[0083] First, based on the first behavior link, one feature combination of behavior feature 1, behavior feature 2, behavior feature 3, ..., and behavior feature n can be formed by using behavior features of behavior record 1, behavior record 2, behavior record 3, ..., and behavior record n.

[0084] Then, based on the second to the fourth behavior links, three feature combinations can be formed by using behavior record 1, behavior record 1A1, behavior record 2, behavior record 2A1, behavior record 3, ..., and behavior record n. The three feature combinations are respectively as follows:

[0085] Feature combination 1: behavior feature 1, behavior feature 2, behavior feature 2A1, behavior feature 3, ..., and behavior feature n.

[0086] Feature combination 2: behavior feature 1, behavior feature 1A1, behavior feature 2, behavior feature 3, ..., and behavior feature n.

[0087] Feature combination 3: behavior feature 1, behavior feature 1A1, behavior feature 2, behavior feature 2A1, behavior feature 3, ..., and behavior feature n.

[0088] For step 206, it is determined whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, it is determined that the applet conducts a malicious behavior.

[0089] In some embodiments of this specification, the feature combination of the malicious behavior record is a feature combination formed based on step 202 to step 204 for a malicious behavior record of a malicious behavior that has been discovered.

[0090] For example, the malicious behavior includes the following three consecutive behaviors: invoking a user camera to photograph -> locally saving a file -> uploading a picture to a server.

[0091] For another example, the malicious behavior includes the following five consecutive behaviors: setting an applet title (xxx chess game) -> enabling a payment interface -> entering a fixed collection account -> obtaining a payment status.

[0092] In some embodiments of this specification, the feature combination of behavior feature 1, behavior feature 2, behavior feature 3, behavior feature 4, behavior feature 5, ..., and behavior feature n is used as an example, and the classification values and sensitivity weight values that are determined in terms of two dimensions in step 202 are all used as behavior features of the behavior record. In such case, the feature combination is (X1, Y1), (X2, Y2), (X3, Y3), (X4, Y4), (X5, Y5), ..., and (Xn, Yn), where Xn is used to represent a classification value of the behavior feature n, and Yn is used to represent a sensitivity weight value of the behavior feature n.

[0093] It is assumed that a feature combination of a known malicious behavior record is (X2, Y2), (X3, Y3), and (X4, Y4). In such case, when it is determined whether the feature combination formed for the applet includes the feature combination of the malicious behavior record, it is necessary to sequentially compare whether behavior features at locations in a one-to-one correspondence are the same. For example, first, it is compared whether three behavior features (X1, Y1), (X2, Y2), and (X3, Y3) in the feature combination formed for the applet are the same as the feature combination of the malicious behavior record, and a comparison result indicates that they are different. Then, it is compared whether three behavior features (X2, Y2), (X3, Y3), and (X4, Y4) in the feature combination formed for the applet are the same as the feature combination of the malicious behavior record, and a comparison result indicates that they are the same. In such case, it can be determined that the feature combination formed for the applet includes the feature combination of the malicious behavior record.

[0094] Detection of a malicious behavior of an applet has been implemented above.

[0095] Some embodiments of another aspect further provide an apparatus for detecting a malicious behavior of an applet. FIG. 7 shows an apparatus for detecting a malicious behavior of an applet according to some embodiments. It may be understood that the apparatus can be implemented by any apparatus, device, platform, or device cluster having computing and processing capabilities. As shown in FIG. 7, the apparatus 70 includes: a behavior record obtaining unit 71, configured to obtain at least two behavior records that are generated through triggering during running of the applet; a behavior feature extraction unit 72, configured to extract a behavior feature of each behavior record; a feature combination unit 73, configured to form at least one feature combination by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features; and a determining unit 74, configured to determine whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, determine that the applet conducts a malicious behavior.

[0096] In some possible implementations, the behavior record includes at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

[0097] In some possible implementations, the behavior record obtaining unit 71 is configured to obtain at least two behavior records generated by the applet during running of the applet; and the feature combination unit 73 is configured to form one feature combination by using behavior features of the at least two behavior records generated by the applet.

[0098] In some possible implementations, the behavior record obtaining unit 71 is configured to: obtain at least two behavior records generated by the applet during running of the applet; for two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determine whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generate a corresponding behavior record for the third function page; and use the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

[0099] In some possible implementations, the feature combination unit 73 is configured to form a first feature combination by using behavior features of the at least two behavior records generated by the applet; and form at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

[0100] In some possible implementations, the behavior record obtaining unit 71 is configured to: when obtaining the at least two behavior records generated by the applet during running of the applet, obtain at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet.

[0101] In some possible implementations, the behavior feature extraction unit 73 is configured to determine, based on a name, included in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determine a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determine the determined classification value as the behavior feature of the behavior record; and/or detect, based on parameter information, included in the behavior record, in an invoking request sent by the applet and parameter information, included in the behavior record, in an invoking request response received by the applet, privacy data included in the parameter information; determine, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determine the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

[0102] Some embodiments of this specification provide a computer-readable storage medium, where the computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the method according to any embodiment of this specification.

[0103] Some embodiments of this specification provide a computing device, including a memory and a processor, where the memory stores executable code, and the processor executes the executable code to implement the method according to any embodiment of this specification.

[0104] It may be understood that the structure illustrated in some embodiments of this specification does not constitute a specific limitation on the apparatus for detecting a malicious behavior of an applet. In some other embodiments of this specification, the apparatus for detecting a malicious behavior of an applet may include more or fewer components than those shown in the figure, or combine some components, or split some components, or have different component arrangements. The components in the figure can be implemented by hardware, software, or a combination of software and hardware.

[0105] Content such as information exchange and an execution process between the modules in the apparatus and the system is based on the same idea as some method embodiments of this specification. Therefore, for detailed content, references can be made to descriptions in the method embodiments of this specification, and details are not described herein again.

[0106] Some embodiments of this specification are described in a progressive way. For same or similar parts of some embodiments, mutual references can be made to the embodiments. Each embodiment focuses on a difference from other embodiments. Particularly, some apparatus embodiments are briefly described since they are basically similar to some method embodiments. For related parts, references can be made to related descriptions in the method embodiments.

[0107] A person skilled in the art should be aware that in the above-mentioned one or more examples, functions described in this specification can be implemented by hardware, software, firmware, or any combination thereof. When these functions are implemented by software, they can be stored in a computer-readable medium or transmitted as one or more instructions or code on the computer-readable medium.

[0108] The above-mentioned some specific implementations further describe the purposes, technical solutions, and beneficial effects of this specification. It should be understood that the foregoing descriptions are merely some specific implementations of this specification and are not intended to limit the protection scope of this specification. Any modification, equivalent replacement, or improvement made based on the technical solutions of this specification shall fall within the protection scope of this specification.

Claims

1. A method for detecting a malicious behavior of an applet, comprising:

   obtaining at least two behavior records that are generated through triggering during running of the applet;
   extracting a behavior feature of each behavior record;
   forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records, wherein each feature combination comprises at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features;
   determining whether there is a feature combination that comprises a predetermined feature

combination of a malicious behavior record; and if there is a feature combination that comprises the predetermined feature combination of a malicious behavior record, determining that the applet conducts a malicious behavior.

2. The method according to claim 1, wherein the behavior record comprises at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

3. The method according to claim 1, wherein

the obtaining at least two behavior records that are generated through triggering during running of the applet comprises: obtaining at least two behavior records generated by the applet during running of the applet; and
the forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records comprises: forming one feature combination by using behavior features of the at least two behavior records generated by the applet.

4. The method according to claim 1, wherein the obtaining at least two behavior records that are generated through triggering during running of the applet comprises:

obtaining at least two behavior records generated by the applet during running of the applet; for two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determining whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generating a corresponding behavior record for the third function page; and
using the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

5. The method according to claim 4, wherein the forming at least one feature combination by using at least two behavior features of at least two successively generated behavior records comprises:

forming a first feature combination by using behavior features of the at least two behavior records generated by the applet; and
forming at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

6. The method according to claim 3 or 4, wherein the obtaining at least two behavior records generated by the applet during running of the applet comprises: obtaining at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet.

7. The method according to claim 1, wherein the extracting a behavior feature of each behavior record comprises:

determining, based on a name, comprised in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determining a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determining the determined classification value as the behavior feature of the behavior record;
and/or
detecting, based on parameter information, comprised in the behavior record, in an invoking request sent by the applet and parameter information, comprised in the behavior record, in an invoking request response received by the applet, privacy data comprised in the parameter information; determining, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determining the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

8. An apparatus for detecting a malicious behavior of an applet, comprising:

a behavior record obtaining unit, configured to obtain at least two behavior records that are generated through triggering during running of the applet;
a behavior feature extraction unit, configured to extract a behavior feature of each behavior record;
a feature combination unit, configured to form at least one feature combination by using at least

two behavior features of at least two successively generated behavior records, wherein each feature combination comprises at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features; and

a determining unit, configured to determine whether there is a feature combination that comprises a predetermined feature combination of a malicious behavior record; and if there is a feature combination that comprises the predetermined feature combination of a malicious behavior record, determine that the applet conducts a malicious behavior.

9. The apparatus according to claim 8, wherein the behavior record comprises at least one of the following: a name of a service interface invoked by the applet, time information when the applet invokes the service interface, parameter information in an invoking request sent by the applet, parameter information in an invoking request response received by the applet, and information about a function page corresponding to the applet after invoking the service interface.

10. The apparatus according to claim 8, wherein

the behavior record obtaining unit is configured to obtain at least two behavior records generated by the applet during running of the applet; and the feature combination unit is configured to form one feature combination by using behavior features of the at least two behavior records generated by the applet.

11. The apparatus according to claim 8, wherein the behavior record obtaining unit is configured to: obtain at least two behavior records generated by the applet during running of the applet; for two adjacent behavior records in the at least two behavior records, when a first function page corresponding to a behavior record with an earlier generation time jumps to a second function page corresponding to a behavior record with a later generation time, determine whether the first function page jumps to the second function page via at least one third function page, and if the first function page jumps to the second function page via at least one third function page, generate a corresponding behavior record for the third function page; and use the at least two behavior records generated by the applet and the behavior record corresponding to the third function page as the at least two behavior records that are generated through triggering during running of the applet.

12. The apparatus according to claim 11, wherein the feature combination unit is configured to form a first feature combination by using behavior features of the at least two behavior records generated by the applet; and form at least one second feature combination by using the behavior features of the at least two behavior records generated by the applet and a behavior feature of the behavior record corresponding to the third function page.

13. The apparatus according to claim 10 or 11, wherein the behavior record obtaining unit is configured to: when obtaining the at least two behavior records generated by the applet during running of the applet, obtain at least two behavior records generated when the applet invokes at least two service interfaces during running of the applet.

14. The apparatus according to claim 8, wherein the behavior feature extraction unit is configured to determine, based on a name, comprised in the behavior record, of a service interface invoked by the applet, a classification of the service interface; determine a classification value corresponding to the classification of the service interface based on a classification value predefined for each classification; and determine the determined classification value as the behavior feature of the behavior record; and/or detect, based on parameter information, comprised in the behavior record, in an invoking request sent by the applet and parameter information, comprised in the behavior record, in an invoking request response received by the applet, privacy data comprised in the parameter information; determine, based on a predetermined mapping relationship between a data type and a sensitivity weight value, a sensitivity weight value corresponding to the privacy data; and determine the sensitivity weight value corresponding to the privacy data as the behavior feature of the behavior record.

15. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when the computer program is executed on a computer, the computer is enabled to perform the method according to any one of claims 1 to 7.

16. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and the processor executes the executable code to implement the method according to any one of claims 1 to 7.

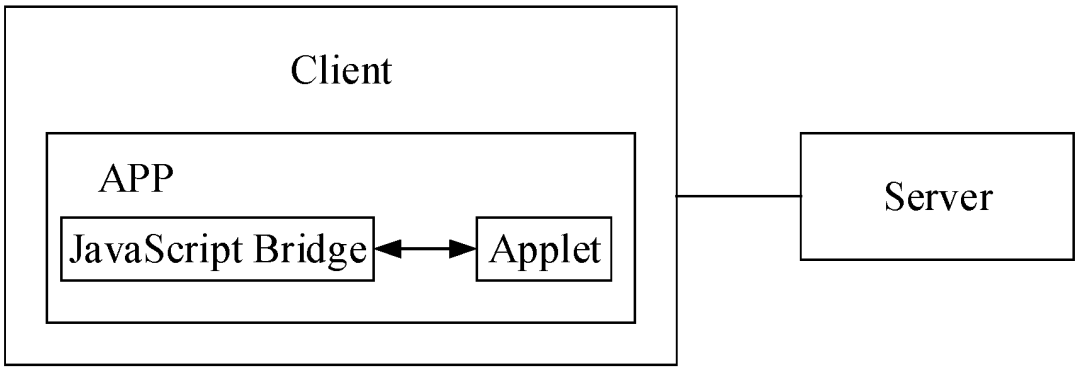
Client
APP
JavaScript Bridge
Applet
Server

FIG. 1

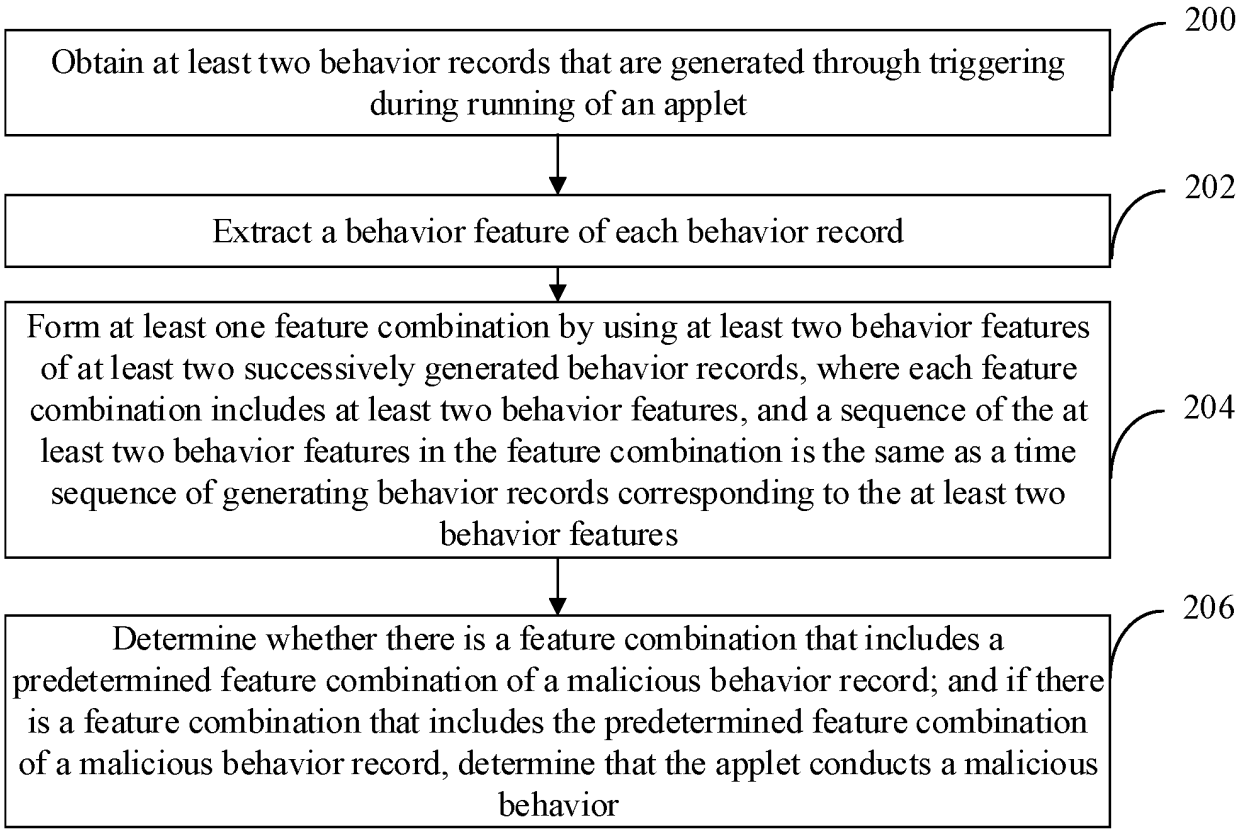
Obtain at least two behavior records that are generated through triggering during running of an applet
200
Extract a behavior feature of each behavior record
202
Form at least one feature combination by using at least two behavior features of at least two successively generated behavior records, where each feature combination includes at least two behavior features, and a sequence of the at least two behavior features in the feature combination is the same as a time sequence of generating behavior records corresponding to the at least two behavior features
204
Determine whether there is a feature combination that includes a predetermined feature combination of a malicious behavior record; and if there is a feature combination that includes the predetermined feature combination of a malicious behavior record, determine that the applet conducts a malicious behavior
206

FIG. 2

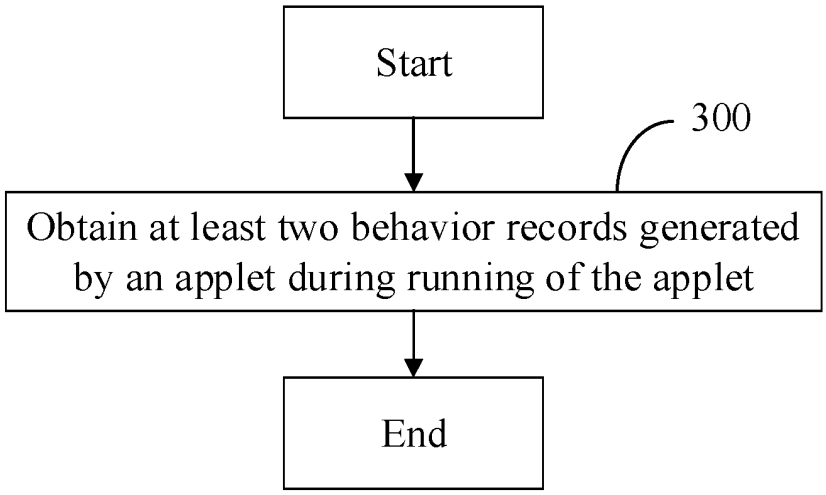

FIG. 3

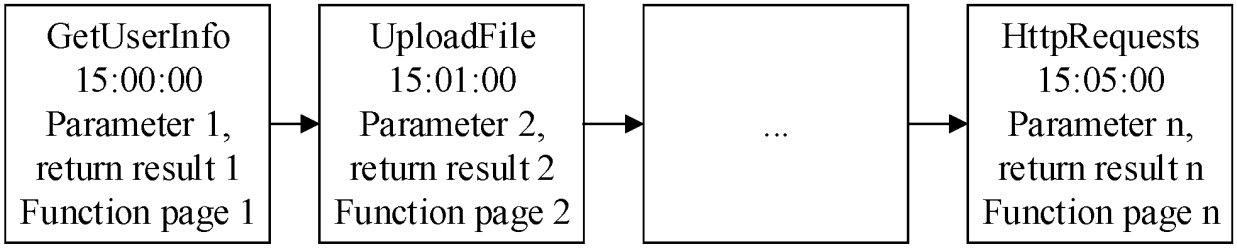

FIG. 4

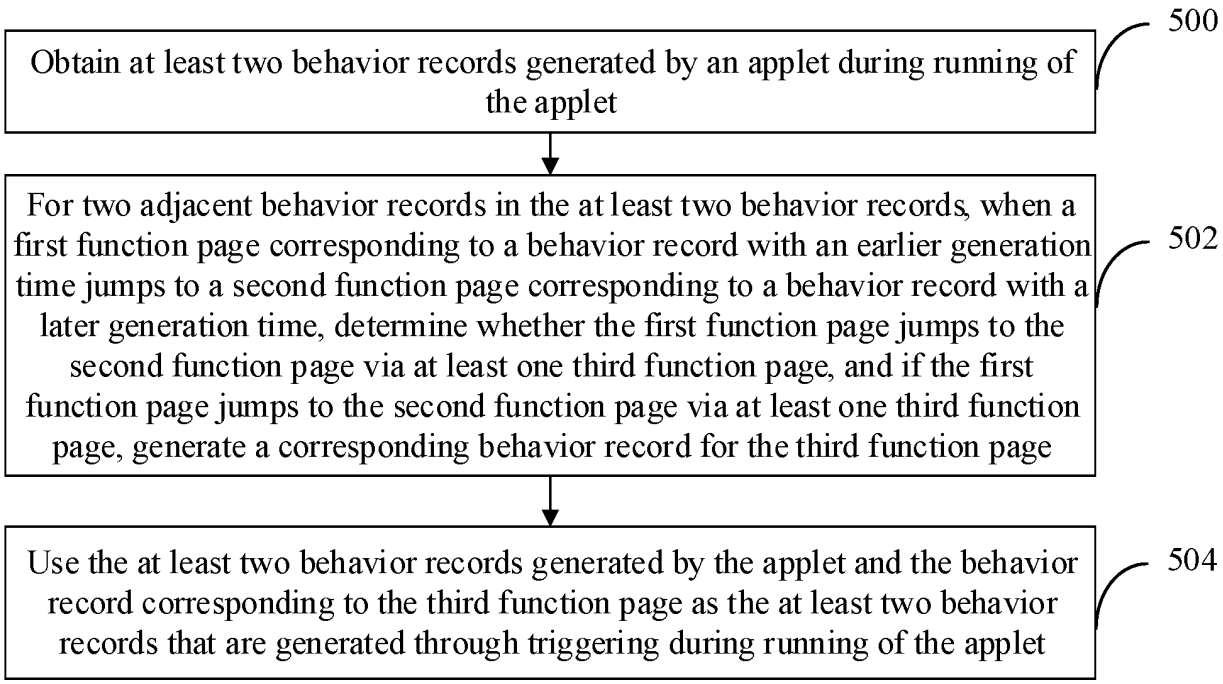

FIG. 5

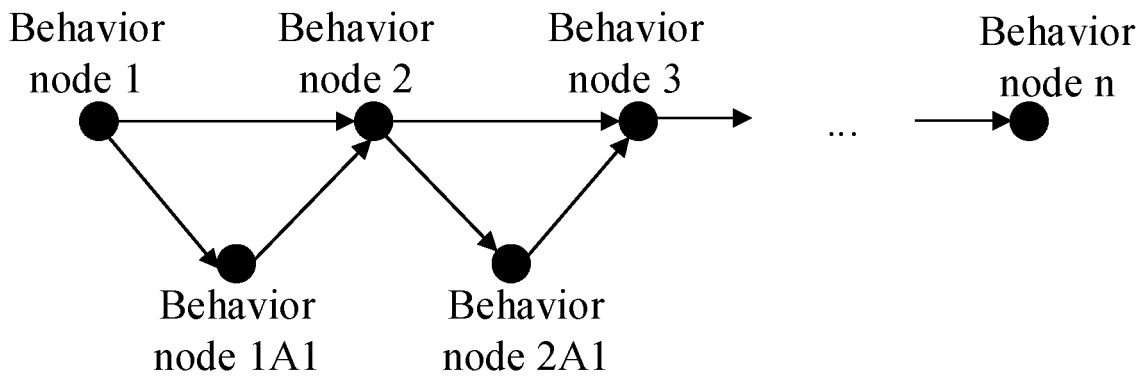
Behavior node 1
Behavior node 2
Behavior node 3
...
Behavior node n
Behavior node 1A1
Behavior node 2A1

FIG. 6

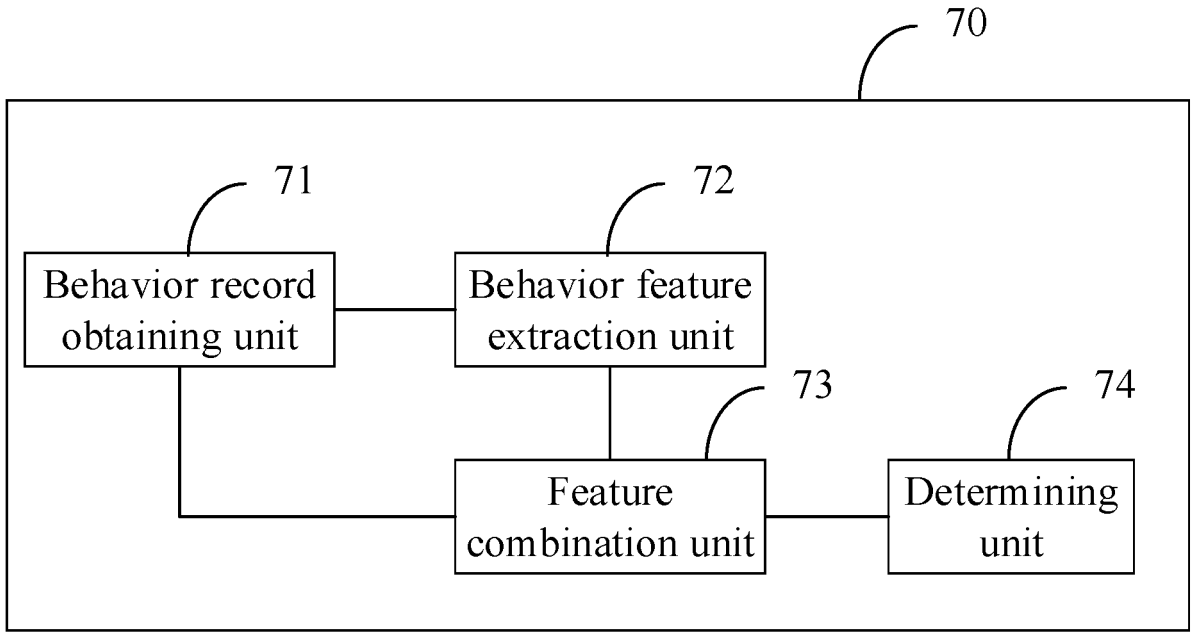
70
71
72
Behavior record obtaining unit
Behavior feature extraction unit
73
74
Feature combination unit
Determining unit

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/076785

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, VEN, USTXT, EPTXT, CNKI: 小程序, 寄宿程序, 寄宿应用, 恶意, 检测, 识别, 行为, 记录, 历史, 序列, 动态行为, 特征, 合并, 组合, 融合, 拼接, 时间戳, 顺序, mini, board, APP, application, malicious, malware, detect+, recogni+, behavior, history, record, chain, sequence, dynamic, feature, character+, combin+, joint, timestamp, temporal, chronologic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113010892 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 22 June 2021 (2021-06-22) description, paragraphs 0051-0150, and figures 1-7	1-16
Y	CN 103761481 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 30 April 2014 (2014-04-30) description, paragraphs 61-84, and figure 1	1-3, 6-10, 13-16
Y	CN 103065093 A (NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY OF PLA) 24 April 2013 (2013-04-24) description, paragraphs 44-53	1-3, 6-10, 13-16
A	CN 104392174 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 04 March 2015 (2015-03-04) entire document	1-16
A	CN 109815701 A (360 ENTERPRISE SECURITY TECHNOLOGY (ZHUHAI) CO., LTD. et al.) 28 May 2019 (2019-05-28) entire document	1-16

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 April 2022	**26 April 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/076785

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017270299 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 21 September 2017 (2017-09-21) entire document	1-16

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/076785

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113010892 A	22 June 2021	None	
CN 103761481 A	30 April 2014	None	
CN 103065093 A	24 April 2013	CN 103065093 B	17 September 2014
CN 104392174 A	04 March 2015	CN 104392174 B	06 April 2016
CN 109815701 A	28 May 2019	None	
US 2017270299 A1	21 September 2017	US 10007789 B2	26 June 2018
		KR 20170108330 A	27 September 2017

Form PCT/ISA/210 (patent family annex) (January 2015)